WHAT IS CLAIMED IS:

1. An IP communication network system:

comprising a plurality of autonomous systems, configuring IP networks of domains independent of each other, for performing interior- and exterior-forwarding of IP packets,

said plurality of autonomous systems including a plurality of border relay devices positioned at borders between the IP networks,

each of said plurality of border relay devices including:

a discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and

a distribution unit for distributing the filtering information to all other border relay devices within said same autonomous system.

2. An IP communication network system according to claim 1, wherein a host computer of each of said plurality of autonomous systems includes a detection unit for detecting based on predetermined items of judging information that the IP packet forwarded is the unauthorized intrusion packet.

3. An IP communication network system according to claim 1, wherein said distribution unit of said border relay device further distributes the filtering information to said border

relay device within said autonomous system facing to said autonomous system from which the unauthorized packet is forwarded.

4. An IP communication network system according to claim 1, wherein each of a plurality of relay devices positioned at relay points between the respective IP networks of said plurality of autonomous systems includes:

a discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and

a distribution unit for distributing the filtering information to all said relay devices within said same autonomous system.

5. A border relay device positioned at a border between autonomous systems, configuring IP networks of independent domains, for performing interior- and exterior- forwarding of an IP packet, said border relay device comprising:

a discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and

a distribution unit for distributing the filtering information to all other border relay devices within said autonomous systems.

6. A border relay device according to claim 5, wherein said distribution unit further distributes the filtering information to said border relay device positioned at a border within said autonomous system facing to said autonomous system from which the unauthorized packet is forwarded.

7. An unauthorized intrusion safeguard method in an IP communication network system having a plurality of autonomous systems, configuring IP networks of independent domains of each other, for performing interior- and exterior-forwarding of IP packets, said method in each of said plurality of autonomous systems, comprising:

detecting that the IP packet forwarded is an unauthorized intrusion packet on the basis of predetermined items of judging information;

discarding the unauthorized packet at one border of the IP network when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and

distributing the filtering information to all other border relay devices within said same autonomous system.

8. An unauthorized intrusion safeguard method according to claim 7, further comprising:

distributing the filtering information to the border within said autonomous system facing to said autonomous system from which the unauthorized packet is forwarded.

9. An unauthorized intrusion safeguard method according to claim 7, further, in each of said plurality of autonomous systems, comprising:

discarding, when the IP packet forwarded is an unauthorized intrusion packet, the unauthorized packet at one border of the IP network when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and

distributing the filtering information to all other relay points within said same autonomous system.

10. An authorized intrusion safeguard method comprising:

discarding, if an IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet at a border between autonomous systems, configuring IP networks of independent domains, for performing interior- and exterior- forwarding of the IP packet; and

distributing the filtering information to all other borders within said autonomous systems.

11. An authorized intrusion safeguard method according

to claim 10, further comprising:

distributing the filtering information to a border within said autonomous system facing to said autonomous system from which the unauthorized packet is forwarded.